REMARKS

Claims 1-28 were pending in the patent application. By this amendment, Applicants have amended the language of all of the independent claims and have added dependent Claim 29. Authorization is hereby given to charge Deposit Account 50-0510 for the addition of one new dependent claim in excess of twenty total claims.

The Examiner has rejected Claims 7, 10-11 and 22-24 under 35 USC 102(e) as being anticipated by Godfrey; Claims 1-2, 5, 8, 1, 19 and 21 under 35 USC 103(a) as being unpatentable over Godfrey in view of Boeyen; Claims 3-4, 6-9, 15, 25 and 27 as being unpatentable over Godfrey in view of Boeyen and further in view of Spelman; Claims 12-16, 26 and 28 as being unpatentable over Godfrey in view of Spelman; and, Claims 18 and 20 as unpatentable over Boeyen in view of Spelman. For the reasons set forth below, Applicants believe that the claims, as amended, are patentable over the cited art.

The present invention provides a system, method, and computer program means for providing digital signing of communications to be transmitted and for providing verification of digital signatures on communications which have been received. The invention provides the digital

signing and signature verification without the need to alter the applications which are generating the communications. Accordingly, the invention provides a proxy server and computer-implemented method at a proxy server whereby a key for creating the digital signature for the communication is selected based on an analysis of the contents of the message document that is being exchanged by the communication, wherein the contents do not include any digital signature data. Once the key has been selected, the digital signature is created for the message document, after which the message document and its digital signature are transmitted. The application which generated the message document/communication in not involved in the creation of the digital signature and need not, therefore, be modified to provide the functionality. Further, for an incoming communication, the proxy server intercepts the communication, selects a public key for verifying the digital signature based on the contents of the message document in the received communication, verifies the digital signature based on the selected public key, and then allows the communication to go to the destination application.

The Godfrey patent is the primary reference cited against the present claims. The Godfrey patent is directed to a system and method for signing markup language data

communicated between first and second units. The signing of the data is done by at least one proxy interposed between the first and second unit. Under Godfrey, the data to be signed includes embedded digital signature initiation data which is detected by the digital signature initiation data detector, 116 of Fig. 1, of the proxy, 108 (see: e.g., Col. 3, lines 34-36 and Col. 4, lines 3-7). The application which generates the markup language data to be signed also generates the digital signature initiation data that tells the proxy to sign the data.

Applicants respectfully assert that the Godfrey patent does not anticipate the invention as set forth in amended Claims 7, 10-11 and 22-24. The claims expressly recite that a key for creating, or for verifying, a digital signature is selected based on the contents of the message document of the communication, wherein said contents do not include any digital signature data. An analysis of the contents of the message document is done by the proxy in order to select the appropriate key for signing, or for verifying, a communication. The analysis is not simply detection of information embedded by an application when the application generated the communication. In fact, as noted above, the present invention expressly provides for digital signing and signature verification without involvement of the

application(s), such that the contents of the message document do not contain any digital signature information.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Godfrey patent does not teach steps or means for creating or verifying a digital signature for a communication/message document, including selecting a key based on the contents of the communication/message document, wherein the contents do not include any digital signature information, and using the key to create or to verify the digital signature, it cannot be maintained that Godfrey anticipates the invention as set forth in the amended claims, Claims 7, 10-11 and 22-24.

Applicants further assert that the claims are patentable over the teachings of Godfrey in view of the additionally-cited art. The Examiner has acknowledged that Godfrey does not teach or suggest more than one key, managing more than one key, or selecting among more than one key. The Examiner has cited the Boeyen patent, stating that Boeyen discloses managing a plurality of private keys to generate a digital signature. The Boeyen patent is directed to an apparatus and method for converting certificates from one format to another format. Under Boeyen, an existing

certificate is accompanied by "desired certificate format criteria data" (see: e.g., the Abstract). When the first certificate with desired certificate format criteria data is received at the certificate converting unit, 24 of Fig. 1, the certificate converting unit simply generates a second certificate in the desired format.

Applicants respectfully assert that the addition of the Boeyen patent teachings to Godfrey would not result in the invention as claimed. Both Godfrey and Boeyen require that the data which is to be processed, the markup language data of Godfrey or the first certificate of Boeyen, be accompanied by "instruction information", the embedded signature initiation data of Godfrey or the desired certificate format criteria data of Boeyen. In contrast, the present invention provides for digital signing and digital signature verification based on message document contents, wherein the contents do not include any digital signature information. As discussed above, under the present invention, the application which generates the communication/message document is not aware of the digital signing and does not have to be altered for the inventive method to be implemented.

Applicants further note that the cited Boeyen teachings from Fig. 6 and 7 and Co. 7, lines 11-14 do not teach or

suggest the claimed key selection rules. What Boeyen describes is an enable/disable signal which prevents a certificate from being generated in any format, wherein the format (i.e., 212a or 212b) is designated by the desired certificate format criteria data. Boeyen does not teach or suggest selection rules or the use of selection rules for key selection based on message document contents.

Since neither reference teaches the claim features, including means and steps for selecting a key based on the contents of the message document, wherein the contents do not include digital signature information, a *prima facie* case of obviousness simply has not been presented by the Examiner *(In re Wilson,* 424 F.2d 1382, 165 USPQ 494 (C.C.P.A. 1970)). Accordingly, Applicants conclude that Claims 1-2, 5, 8, 17, 19 and 21 are not rendered obvious by the combination of Godfrey and Boeyen.

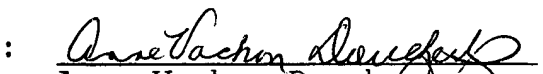
The Examiner has further cited the Spelman patent, in various combinations with Godfrey and/or Boeyen in rejecting the remaining claims. The Spelman patent is cited for its teachings related to using a replacement key if a central authority's root key/private key has been compromised. Applicants respectfully assert that the addition of the Spelman patent teachings would not render the present claims unpatentable. Spelman does not provide those teachings

which are missing from Godfrey, Boeyen, or the combination of Godfrey and Boeyen. Moreover, Spelman simply provides for the generation of a new key (see: e.g., Col. 4, line 65-Col. 5, line 8), which is neither based on the contents of the data to be communicated nor is it related to the satisfaction of key selection rules set for the key which has been selected based on those contents. Clearly, the addition of the teachings of the Spelman patent to the cited art does not result in the invention as claimed.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

H. Maruyama, et al

By: 

Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910